

**Notice of Allowability**

Application No.

09/895,498

Examiner

Eleni A. Shiferaw

Applicant(s)

MAGDYCH ET AL.

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 07/21/2006.
2. ☒ The allowed claim(s) is/are 1,2,4-9,11-20,22-27 and 29-39.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some\* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.  
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08),  
Paper No./Mail Date \_\_\_\_\_
4. ☐ Examiner's Comment Regarding Requirement for Deposit  
of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413),  
Paper No./Mail Date 8/9/06.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_.

**NASSER MOAZZAM**  
**PRIMARY EXAMINER**

DETAILED ACTION

**EXAMINER'S AMENDMENT**

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Kevin J. Zilka on August 9, 2006.

Examiner initiated interview has been made with Kevin J. Zilka to incorporate allowable features, "wherein the at least one of the procedures further includes analyzing responses to the first and second requests", into all base claims, and Kevin J. Zilka agreed to the changes.

2. Examiner amends claims 1, 13-14, 18, 31-32, and 36-38 cancels claims 12 and 30.
  1. (Currently Amended) A method for detecting modifications to risk assessment scanning caused by an intermediate device, comprising:
    - (a) initiating a risk assessment scan at and on a target, from a remote source utilizing a network;
    - (b) determining whether the risk assessment scan at and on the target involves an intermediate device coupled between the target and the remote source;

- (c) receiving results of the risk assessment scan from the target utilizing the network; and
- (d) notifying an administrator if it is determined that the risk assessment scan at and on the target involves the intermediate device, wherein additional operations are carried out to improve a risk assessment at and on the target in view of the presence of the intermediate device coupled between the target and the remote source; wherein a plurality of procedures are utilized to determine whether the risk assessment scan involves the intermediate device; wherein at least one of the procedures includes transmitting a first request for content to the target utilizing the network, and transmitting a second request for a cached version of the content to the target utilizing the network~~(\)~~; and wherein at least one of the procedures further includes analyzing responses to the first and second requests.

12. (Canceled)

13. (Currently Amended) The method as recited in claim ~~12~~ 1, wherein the at least one of the procedures further includes indicating that the risk assessment scan involves the intermediate device based on the analysis.

14. (Currently Amended) The method as recited in claim ~~13~~ 1, wherein the at least one of the procedures further includes indicating that the risk assessment scan involves the intermediate device if the responses to the requests are different.

18. (Currently Amended) A computer program product for detecting modifications to risk assessment scanning caused by an intermediate device, comprising:
- (a) computer code for initiating a risk assessment scan at and on a target, from a remote source utilizing a network;
  - (b) computer code for determining whether the risk assessment scan at and on the target involves an intermediate device coupled between the target and the remote source;
  - (c) computer code for receiving results of the risk assessment scan from the target utilizing the network; and
  - (d) computer code for notifying an administrator if it is determined that the risk assessment scan at and on the target involves the intermediate device;
- wherein additional operations are carried out to improve a risk assessment at and on the target in view of the presence of the intermediate device coupled between the target and the remote source;
- wherein a plurality of procedures are utilized to determine whether the risk assessment scan involves the intermediate device;
- wherein at least one of the procedures includes transmitting a first request for content to the target utilizing the network, and transmitting a second request for a cached version of the content to the target utilizing the network~~(.)~~; and
- wherein at least one of the procedures further includes analyzing responses to the first and second requests.

30. (Canceled)

31. (Currently Amended) The computer program product as recited in claim ~~30~~1, wherein the at least one of the procedures further includes indicating that the risk assessment scan involves the intermediate device based on the analysis.

32. (Currently Amended) The computer program product as recited in claim ~~31~~1, wherein the at least one of the procedures further includes indicating that the risk assessment scan involves the intermediate device if the responses to the requests are different.

36. (Currently Amended) A system for detecting modifications to risk assessment scanning caused by an intermediate device, comprising:

- (a) logic for initiating a risk assessment scan at and on a target, from a remote source utilizing a network;
- (b) logic for determining whether the risk assessment scan at and on the target involves an intermediate device coupled between the target and the remote source;
- (c) logic for receiving results of the risk assessment scan from the target utilizing the network; and
- (d) logic for notifying an administrator if it is determined that the risk assessment scan at and on the target involves the intermediate device;

wherein additional operations are carried out to improve a risk assessment at and on the target in view of the presence of the intermediate device coupled between the target and the remote source;

wherein a plurality of procedures are utilized to determine whether the risk assessment scan involves the intermediate device;

wherein at least one of the procedures includes transmitting a first request for content to the target utilizing the network, and transmitting a second request for a cached version of the content to the target utilizing the network(·); and

wherein at least one of the procedures further includes analyzing responses to the first and second requests.

37. (Currently Amended) A method for detecting modifications to risk assessment scanning caused by a proxy server, comprising:
- (a) initiating a risk assessment scan at and on a target, from a remote source utilizing a network;
  - (b) executing a plurality of procedures to determine whether the risk assessment scan at and on the target involves a proxy server coupled between the target and the remote source;
  - (c) said procedures utilizing a plurality of parameters selected from the group consisting of an ip ttl flag, a tcp\_win flag, a via tag, and a host header value;
  - (d) receiving results of the risk assessment scan from the target utilizing the network;

- (e) flagging the results of the risk assessment scan if at least one of the procedures indicates that the risk assessment scan involves a proxy server coupled between the target and the remote source; and
- (f) notifying an administrator if the results of the risk assessment scan at and on the target are flagged;  
wherein additional operations are carried out to improve a risk assessment at and on the target in view of the presence of the proxy server coupled between the target and the \ remote source;  
wherein at least one of the procedures includes transmitting a first request for content to the target utilizing the network, and transmitting a second request for a cached version of the content to the target utilizing the network(\.); and  
wherein at least one of the procedures further includes analyzing responses to the first and second requests.

38. (Currently Amended) (Currently Amended) A computer program product for detecting modifications to risk assessment scanning caused by a proxy server, comprising:
- (a) computer code for initiating a risk assessment scan at and on a target, from a remote source utilizing a network;
  - (b) computer code for executing a plurality of procedures to determine whether the risk assessment scan at and on the target involves a proxy server coupled between the target and the remote source;
  - (c) said procedures utilizing a plurality of parameters selected from the group consisting

- of an ip\_ttl flag, a tcp\_win flag, a via tag, and a host header value;
- (d) computer code for receiving results of the risk assessment *scan from* the target utilizing the network;
  - (e) computer code for flagging the results of the risk assessment scan if at least one of the procedures indicates that the risk assessment scan involves a proxy server coupled between the target and the remote source;
  - (f) computer code for notifying an administrator if the results of the risk assessment scan at and on the target are flagged;
- wherein additional operations are carried out to improve a risk assessment at and on the target in view of the presence of the proxy server coupled between the target and the remote source;
- wherein at least one of the procedures includes transmitting a first request for content to the target utilizing the network, and transmitting a second request for a cached version of the content to the target utilizing the network(.); and
- wherein at least one of the procedures further includes analyzing responses to the first and second requests.

***Allowable Subject Matter***

3. The following is an examiner's statement of reasons for allowance:

Claims 1-2, 4-9, 11-20, 22-27, and 29-39 are allowed.

Claims 1, 18, and 36-38: Prior art of record neither alone nor in combination teach a method/product/system for detecting modifications to risk assessment scanning caused by an



intermediate device, comprising initiating a risk assessment scan at and on a target, from a remote source utilizing a network; determining whether the risk assessment scan at and on the target involves an intermediate device coupled between the target and the remote source; receiving results of the risk assessment scan from the target utilizing the network; and performing plurality of procedures to determine whether the risk assessment scan involves the intermediate device; wherein at least one of the procedures includes transmitting a first request for content to the target utilizing the network, and transmitting a second request for a cached version of the content to the target utilizing the network, analyzing responses to the first and second requests and indicating that the risk assessment scan involves the intermediate device if the response to the request are different.

Claims 2, 4-9, 11, 13-17, 19-20, 22-27, 29, 31-35 and 39 are allowed because of dependency.


Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

E.S

  
August 9, 2006

**NASSER MOAZZAMI**  
**PRIMARY EXAMINER**

  
8/9/06